SYSTEM AND METHOD FOR EXTENDING SECURE AUTHENTICATION USING UNIQUE SESSION KEYS DERIVED FROM ENTROPY GENERATED BY AUTHENTICATION METHOD

Inventors: Prasanna J. Satarasinghe
2208 Crockett Court
McKinney, TX 75070
Country of Citizenship: Australia

Martin Greenwood
2050 Grayson Drive 8204
Grapevine, TX 76051
Citizenship: United Kingdom

Yoon Hee Kim
712 Greenway Dr.
Coppell, TX 75019
Country of Citizenship: USA

David Ka-Wai Hui
4166 Sora Common
Fremont, CA 94555
Country of Citizenship: Canada

Vlad Alperovich
18419 Rain Dance Trail
Dallas, TX 75252
Country of Citizenship: USA

Assignee: Transat Technologies Inc.
180 State Street, Suite 209
Southlake Town Square
Southlake, Texas 76092

HAYNES AND BOONE, L.L.P.
901 Main Street, Suite 3100
Dallas, Texas 75202-3789
(214) 651-5000

Attorney. Docket No. 31426.51

EXPRESS MAIL NO.: EV333441865US DATE OF DEPOSIT: April 9, 2004

This paper and fee are being deposited with the U.S. Postal Service Express Mail Post Office to Addressee service under 37 CFR §1.10 on the date indicated above and is addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

Karen L. Underwood
Name of person mailing paper and fee

Karen L. Underwood
Signature of person mailing paper and fee

SYSTEM AND METHOD FOR EXTENDING SECURE AUTHENTICATION USING UNIQUE SESSION KEYS DERIVED FROM ENTROPY GENERATED BY AUTHENTICATION METHOD

PRIORITY CLAIM AND RELATED APPLICATION

[0001] This application claims priority of provisional applications entitled "SYSTEM AND METHOD FOR GPRS AUTHENTICATION IN A RADIUS ACCESS CONTROL ENVIRONMENT" and "SYSTEM AND METHOD FOR RADIUS BILLING FOR WIRELESS COMMUNICATION NETWORKS," both of which were filed on April 11, 2003, commonly assigned, and incorporated herein by reference in their entirety. In addition, this application is related to U.S. Application Serial No. 09/851,681, filed on May 8, 2001, which is commonly assigned and incorporated herein by reference in its entirety.

BACKGROUND

[0002] The present invention relates generally to communications systems and more particularly, to a system and method for utilizing existing communications networks.

[0003] With the advancement of telecommunication technologies, subscriber identity modules (SIMs), also known as a type of smart cards, are becoming increasingly prevalent for wireless customers. However, legacy communications networks, such as a public wireless local area network (PWLAN), may be unable to provide network access to customers based on their SIMs.

[0004] Accordingly, it is desired to provide a means for SIM users to access the PWLANs in a secured environment and to allow an unified accounting scheme.

[0005] It is also desired to provide a cost effective solution, so that extensive modifications will not be required for the existing PWLANs.

BRIEF DESCRIPTION OF THE DRAWINGS

[0006] Fig. 1 illustrates a simplified communications system according to one embodiment of the present disclosure.

[0007] Fig. 2 illustrates a method for utilizing existing communications networks according to one embodiment of the present disclosure.

[0008] Fig. 3 illustrates a system for implementing the method of Fig. 2 according to one embodiment of the present disclosure.

[0009] Figs. 4A-4B illustrate one form of accounting information according to one embodiment of the present disclosure.

[00010] Fig. 5 illustrates a message flow system according to one embodiment of the present disclosure.

DETAILED DESCRIPTION

[00011] For the purposes of promoting an understanding of the principles of the invention, references will now be made to the embodiments, or examples, illustrated in the drawings and specific languages will be used to describe the same. It will nevertheless be understood that no limitation of the scope of the invention is thereby intended. Any alterations and further modifications in the described embodiments, and any further applications of the principles of the invention as described herein, are contemplated as would normally occur to one skilled in the art to which the invention relates.

[00012] The present disclosure relates generally to the field of communications systems, and more particularly, to a system and method for utilizing existing communications networks.

[00013] The current disclosure may be utilized in the following example: a laptop equipped with a subscriber identity module (SIM) attempts to access a traditional public wireless local area

network (PWLAN). However, since the PWLAN includes a typical remote authentication dial-in client services (RADIUS) authentication, authorization, and accounting (AAA) server that is unable to authenticate the laptop based on the SIM, the laptop is unable to access the PWLAN. Therefore, it is desired to provide an adapter system that facilitates the communication between the laptop and the PWLAN.

[00014] Referring now to Fig. 1, shown therein are selected components of a communications system 10 according to one embodiment of the present disclosure. In this example, a client 20, which may be a laptop computer equipped with a device 22, which may contain an international mobile subscriber identity (IMSI), may attempt to access a server 24, which may be a RADIUS AAA server. However, the server 24 is unable to authenticate the client 20 based on the IMSI. Accordingly, the present disclosure provides an adapter 26, which may be used to facilitate the communication between the client 20 and the server 24.

[00015] Referring now to Fig. 2, shown therein is a method 100 for facilitating the communication between the client 20 and the server 24 according to one embodiment of the present disclosure. In this embodiment, the method 100 may assist the authentication and/or billing of the client 20 in the PWLAN environment. Step 102 of the method 100 creates a password for the client 20, step 104 of the method 100 utilizes the password and a client id to authenticate the client, and step 106 of the method modifies accounting data of the client 20. The method 100 will be further described below in connections with Fig. 3.

[00016] Referring now to Fig. 3, shown therein is an implementation of the methods 100 according to one embodiment of the present disclosure. In this embodiment, a network 200 may include the client 20, which may comprise or may be connected to the device 22, an access controller 202, the server 24, the adapter 26, a signaling gateway 206, and a home location register (HLR) 208.

[00017] Here, the client 20 may comprise a computing device such as a personal computer, personal digital assistant, pager, cellular telephone, and the like. For the sake of example, the client 20 may include a central processing unit (CPU), a memory unit, an input/output (I/O) device, and an external interface. The external interface may be, for example, a modem, a wireless transceiver, and/or one or more network interface cards (NICs). It is understood that the

client 20 may be differently configured and that each of the listed components may actually represent several different components. For example, the CPU may represent a multi-processor or a distributed processing system; the memory unit may include different levels of cache memory, main memory, hard disks, and remote storage locations; and the I/O device may include monitors, keyboards, and the like.

[00018] In furtherance of the example, the device 22 may include a Subscriber Identity Module (SIM) card, universal SIM card, any other smart card, or any other means for identifying the client 20. In one example, the SIM card may include an IMSI or other identification devices. The SIM card is included in each mobile phone that conforms to the global system for mobile communications (GSM) and many personal communications services (PCS) handsets. Each SIM card contains a microchip that houses a microprocessor with on-board memory. The SIM card also identifies the caller to the mobile network as being a legitimate caller. The SIM card may resemble a credit card that can be inserted into the client 20, or it may be an integral part of the client 20.

[00019] The access controller 202 may be a system that provides secure access to services, resources, data, telephone switches or LANs. It may provide access control and routing functionality to a device, such as the client 20, through access points (not shown) and other network routing devices.

[00020] The server 24 may provide authentication services to determine the identity of a client attempting to access the PWLAN. It may comprise a Remote Authentication Dial-In User Service (RADIUS) server or any other servers. RADIUS is an authentication and accounting system used by many internet service providers (ISP) and end user organizations to provide secure Internet access, especially in a Virtual Private Networks (VPN) application. When the ISP is dialed, user name and password must be entered and passed to a RADIUS server, which verifies the information, and then authorizes access to the ISP systems and network. RADIUS is a client/server-based authentication software system that centralizes the administration of user profiles maintained in authentication databases.

[00021] The adapter 26 may comprise one or more software programs written in a high-level and/or standard programming language, such as C, C++, or Java. It may be utilized to

authenticate the client 20, provide PWLAN access to the client 20, and/or manage and deliver accounting data. In one example, the adapter 26 may include one or more of the following application programs, each of which may be written in a high-level and/or standard language, such as C, C++, Java, or other languages:

General Packed Radio Server (GPRS)/Global System for Mobile Communications (GSM) Authentication Application: it may manage client authentication based on GPRS or GSM.

Extensible Authentication Protocal (EAP)-SIM Authentication Application: it may manage client authentication based on EAP-SIM.

Password Application: it may generate a password for the client.

Mobile Application Part (MAP) over Internet Protocol (IP) Inter-working: it may communicate with the HLR 208 to fetch subscriber information.

Database: it may store identification information and a password for the client 20.

Transport for SIM Based Application: it may serve as a transport for authentication messages between the client 20 and the adapter 26.

Accounting Application: it may manage call detail recording (CDR) based accounting upon receiving RADIUS accounting messages.

SIM Gateway Application: when the adapter 26 is configured as a gateway server, it may transfer the EAP-SIM authentication messages received on the transport layer to the remote AAA EAP-SIM server in the client 20's home network.

[00022] The signaling gateway 206 may provide signaling system 7 (SS7) or SS7 over IP standard for communication between the adapter 26 and the HLR 208. SS7 typically employs a

dedicated 64 kilobit data circuit to carry packetized machine language messages about each call connected between and among machines of a network to achieve connection control. The signaling gate way 206 may provide the following functions: supervising—it may monitor the status of a line or circuit to see if it is busy, idle or requesting services; alerting—it may indicate the arrival of an incoming call by signals such as bells, buzzers, whoofers, tones, strobes and lights; and addressing—it may transmit routing and destination signals in the form of dial pulses, tone pulses or data pulses over loops, trunks and signaling networks.

[00023] The HLR 208 may comprise a database that holds subscription information and authentication triples of every subscriber in the network. The HLR 208 may be a permanent SS7 database used in cellular networks, such as Advanced Mobile Phone system (AMPS), GSM and PCS. The HLR 208 may be located on the Signal Control Point (SCP) of the cellular provider of record, and may be used to identify/verify a subscriber, and/or store subscriber data related to features and services. In a roaming scenario, the local service provider queries the HLR 208 via a SS7 link. Once verified, client data is transferred via SS7 to and maintained at the Visitor Location Register (VLR) during the period of roaming activity within the coverage area of the provider.

[00024] The method 100 will now be further described. Referring to Figs. 2 and 3, in an exemplary operation of the method 100, the client 20 may comprise an application program (not shown), which may be written in any standard language, such as C, C++, or Java. According to methods known in the art, the application program may enable the client 20 to search for and identify the adapter 26 and initiate an authentication request through the access controller 202 by providing its identification information, which may be an IMSI, contained in the device 22. As a result, the access controller 202 may forward the identification information to the adapter 26, which may in turn convey the identification information to the HLR 208 for authentication.

[00025] In furtherance of the example, once the HLR 208 has authenticated the identification information supplied by the client 22, it may send a success message to the adapter 26, which may notify the client 20 of the successful completion of the authentication. Then, an application program (not shown) residing on the adapter 26 may generate an one-time password for use in connection with the RADIUS authentication described below. Independently, an application

program (not shown) residing on the client may also generate an identical password for the client 20.

[00026] The process of generating the password for the client 20 is now further described. In one embodiment, the password may be generated based on information that identifies the client 20, such as the IMSI, a pseudonym, or any other information that identifies the client 20. In one example, the password may be derived as follows:

password = F (generating a hash value (Username | n*Value | "sim direct"))

Username: comprises the identification information of the client 20, such as a pseudonym, a permanent identity (which may be IMSI), or any other information that is associated with the client 20.

n: a digital number.

Value: comprises Kc, which is a 64-bit ciphering key known in the art; MicroSoft - Microsoft Point-to-Point Encryption (MS-MPPE)-Send-Key; MS-MPPE-Recv-Key; or any other value that is suitable for generating the password.

n*Value: represents concatenating n number of Values together.

sim direct: comprises the character string of "sim direct".

F: represents a function that converts a hash value into an alpha-numeric string.

For example, the following octet values may be used:

H'30-H'39 (decimal 48-57), which may be represented by the values of 0 to 9.
H'41-H'5A (decimal 65-90), which may be represented by the values of A to Z.
H'61-H'7A (decimal 97-122), which may be represented by the values of a to z.

The F function may be used to convert other values into the value ranges listed above. For example, F may perform the following functions:

if an octet value ranges from 0 through 23,
add 65 to the octet value;

if an octet value ranges from 24 through 47,
add 41 to the octet value;

if an octet value ranges from 58 through 64,
add 10 to the octet value;

if an octet value ranges from 91 through 96,
add 6 to the octet value;

if an octet value ranges from 123 through 144,
subtract 26;

if an octet value ranges from 145 through 165,
subtract 46;

if an octet value ranges from 166 through 185,
subtract 66;

if an octet value ranges from 186 through 205,
subtract 86;

if an octet value ranges from 206 through 225,
subtract 106;

if an octet value ranges from 226 through 245;
subtract 126;

if an octet value ranges from 246 through 255;
subtract 146.

The resulting stream may be used as the password for the client 20.

[00027] In the above descriptions, the hash value may be generated pursuant to hashing techniques. However, it is understood that any other value that is capable of uniquely identifying the client may also be utilized. The hash value may be generated using any of a variety of high entropy, less colliding techniques, such as a Secure Hash Algorithm (e.g., SHA-1), a Message Digest Algorithm (e.g., MD5), or a variation of the RACE Integrity Primitives Evaluation (e.g., RIPEMD-160) techniques. The various standards for the hashing methods are known in the art. For example, the standard for SHA-1 is described in the Federal Information Processing Standards Publication 180-1 (FIPS PUB 180-1) dated April 17, 1995, and issued by the National Institute of Standards and Technology, which is hereby incorporated by reference.

[00028] It is contemplated that many variations of the above example may be applied to derive the password. In one example, the string "sim direct" may not be utilized or may be replaced by another string. In a second example, n may not be utilized. In a third example,

Value may not be utilized. In a fourth example, instead of generating a hash value, other algorithms or methods may be adopted to create the password. In a fourth example, the function F may not be utilized, or may be modified. Accordingly, a variety of means may be utilized for generating the password for the client 20.

[00029] In furtherance of the example, once the application program residing on the adapter 26 has successfully generated the password, the application program (or another program) may transfer the Username and the password of the client 20 to the server 24. As a result, the server 24 may store the information in a database or on a list. Then, the adapter 26 may notify the client 20 of the generation of the password, and may convey any suitable information (such as the pseudonym of the client 20) to the client 20. Since the client 20 may access identical algorithms or methods for generating the password, an application program residing on the client 20 may proceed to generate an identical password, using the procedures described above. Then, the application program (or another program) residing on the client 20 may initiate an authentication process with the server 24 through the access controller 202, utilizing the Username and the password of the client 20. Since the Username and the password have already been stored on the server 24, the server 24 is able to complete the authentication of the client 20 by matching the Username and the password with what have been stored on the server 24.

[00030] In furtherance of the example, upon the successful completion of the authentication process, the access controller 202 will allow the client to access the PWLAN according to methods known in the art. Later, when the access between the client 20 and the PWLAN is terminated by conventional methods, the adapter 26 may intercept the termination message. As a result, an application program residing on the adapter 26 may extract accounting data from the server 24, and modify the data to conform to general standard accounting records for Global System for Mobile Communications (GSM), General Packet Radio Service (GPRS) (for example, Call Detail Records (CDR)), or other systems. Referring now to Figs. 4A and 4B, shown therein is a table comprising additional fields that may be inserted into RADIUS based accounting data for converting them into GPRS based accounting data according to one embodiment of the present disclosure. In that example, a Charging Data Record (CDR) filed 212 may represent fields that may be inserted into RADIUS based accounting data, a Presence column 214 may represent the conditions for the corresponding CDR fields, a Description

column 216 may describe the corresponding CDR fields, and a Source column 218 may identify the source for the corresponding CDR fields. Also the following abbreviations are also used in connections with Figs. 4A and 4B:

GGSN: represents Gateway GPRS Support Node.

SGSN: represents Gateway Serving GPRS Support Node.

PDP: represents Gateway Packet Data Protocol.

APN: represents Gateway Access Point Name.

NI: represents Gateway Network Identifier.

AP: represents Gateway Access Point.

[00031] In addition, upon the termination of the access, both the server 24 and the adapter 26 may erase the stored Username and the password of the client 20.

[00032] It is contemplated that may variations of the above example may be utilized for the present disclosure. In one example, instead of an adapter 26 that is utilized for both the initial authentication of the client 20 and the subsequent generation of the password for the client 20, separate entities may be utilized to perform the functions. In a second example, an existing device may be utilized to authenticate the client 20 through the HLR 208 , and a separate device may be utilized to interact with the existing device and generate the password for the client 20.

[00033] Referring now to Fig. 5, shown therein is a message flow system for implementing the method 100 according to another embodiment of the present disclosure. As many of the details have already be described in the previous embodiment in connections with Figs. 3, 4A and 4B, only brief descriptions will be provided herein. In this example, the adapter 26 may comprise a wireless access internet node (WAIN) server, and the authentication system may comprise extensible authentication protocol (EAP)-SIM authentication.

[00034] In furtherance of the example, the client 20 may initiate the EAP-SIM authentication using a transport protocol, such as radius link adaptation (RLA) in the visited network. The client 20 may utilize a username, such as imsi@realm, or pseudonym@realm. Then, the WAIN

server 302 may recognize that the authentication request should be fulfilled by the remote EAP-SIM server 304, which may be another WAIN server or a third-party EAP-SIM server. Upon the successful authentication by the remote EAP-SIM server 304 pursuant to methods known in the art, the remote EAP-SIM server 304 may send Access Accept packet with EAP-Success and WEP keys (MS-MPPE-Send-Key, and MS-MPPE-Recv-Key), which are known in the art, to the WAIN server 302. Then, the WAIN server 302 may generate a password using the following algorithm:

Password = F (SHA-1 (Username | n*MS-MPPE-Send-Key | "sim gateway"))

Username: it may be identical to the client identity used in the authentication procedure, and may comprise a pseudonym, or a permanent identity, such as IMSI, of the client 20.

n*MS-MPPE-Send-Key: it may comprise n number of MS-MPPE-Send-Key values concatenated together; while n may be determined during the authentication procedure.

sim gateway: it may comprise the character string "sim gateway".

F: it may represent a function of converting a hash value into an alpha-numeric string, which has been described in connections with Fig. 3.

[00035] In furtherance of the example, once the password is generated, the WAIN server 302 may store Username and the password of the client 20 in a RADIUS database residing on the RADIU server 24. Then, an EAP-Succss message may be sent to the client 20, which may generate an identical password. During the process, MS-MPPE-Send-Key and MS-MPPE-Recv-Key may both be generated at the client 20, using key materials exchanged during the EAP-SIM authentication. Once the password is generated by an application program residing on the client 20, the client 20 may perform a http post to log in to the access controller 202 with Username and the password. Thereafter, the access controller 202 may send RADIUS Access Request packet to the RADIUS server 24, which in turn may authenticate the client 20.

[00036] Although only a few exemplary embodiments of this invention have been described in detail above, those skilled in the art will readily appreciate that many modifications are possible in the exemplary embodiments without materially departing from the novel teachings and advantages of this invention. Also, features illustrated and discussed above with respect to some embodiments can be combined with features illustrated and discussed above with respect to other embodiments. Accordingly, all such modifications are intended to be included within the scope of this invention.